HORIZON 2020

Secure Societies

Stefanos Vrochidis

Centre for Research and Technology Hellas

Ioannis Kotsiopoulos

Dotsoft S.A.

TURKEY in HORIZON 2020

EUROPEAN COMMISSION

HORIZON 2020

INNOVATION UNION

Call - SECURITY - Fight against crime and Terrorism

- SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

- SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories

- SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks

- SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

Challenge: The European Union must prevent, and if necessary investigate and mitigate the impact of criminal acts, whilst protecting fundamental rights of its citizens.

Scope

- The definition of a European Security Model which builds upon the analysis of the human factors, at the roots of the design of security strategies and methodologies.

- The globalization of communications allows for cybercrime to develop, and corruption and financial crime to take new forms and use new tools. Law Enforcement Agencies need new equipment to counter such developments.

Proposals should address only one of the following aspects (sub-topics):

1. New methods for the protection of crowds during mass gatherings;

2. New methods to prevent, investigate and mitigate cybercriminal behaviours;

3. New methods to prevent, investigate and mitigate corruption and financial crime to fight the infiltration of organised crime in the European Union (licit) economy;

4. New methods to prevent, investigate and mitigate high impact petty crimes;

5. New methods to prevent, investigate and mitigate high impact domestic violence.

SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

Expected impact

- A policy-making toolkit to advance towards a future European Security Model applicable by European law enforcement agencies

- Common long-term approaches for assessing threats and identifying security measures, including through acceptance tests and cost-benefit considerations

- Complementing the relevant work of Eurobarometer, better understanding of how the citizens perceive security and how it affects their feeling of insecurity, and in connection with potential limitations to, or risks of violations of privacy, and the consequent challenges for LEAs;

- Toolkits for law enforcement agencies, based and validated against the needs and requirements expressed by practitioners, and improving the perception by the citizens that Europe is an area of freedom, justice and security.

SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

Topic conditions

- Practitioners from various disciplines, including a minimum of 5 LEAs from 5 EU Member States or Associated Countries, must be beneficiaries of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant.

- Please note that this topic is planned to be opened also in 2017 with an indicative opening date of 01/03/2017 and an indicative deadline of 24/08/2017, subject to a separate financing decision for 2017

Type of action: RIA Research and Innovation action

Deadline Model: single-stage

Indicative budget: 3M€

Deadline: August 24, 2017

SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories

Challenge: EU vision about European Forensic Science 2020 (European Council conclusions)

Scope

- The most promising forensic techniques need to be developed further, and brought up from experiment to a toolkit usable on a daily basis across Europe. EU Forensic laboratories have to agree on common technical standards and join forces along the following steps:

- Phase 0: To prepare an inventory of forensic technologies already available at TRL 4 or 5, and to identify, within all areas covered by the various ENFSI working groups (http://www.enfsi.eu/), a subset of technologies to be brought at TRL 8;

- Phase 1: To prepare the tenders to build prototypes of a toolkit integrating the above-mentioned subset of technologies, that can be used across Europe; To develop EU-wide benchmarks and validation methods for forensic technologies;

- Phase 2: To implement the calls for tenders to generate 2 prototype toolkits;

- Phase 3: To validate the 2 toolkits against the methods developed during Phase 1;

- Phase 4: To draft a curriculum for pan European training in forensic technologies, and to plan for its assessment across Europe; to initiate the EU-wide certification of the toolkits based on the results of Phase 3.

SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories

Expected impact

Medium term:

- Advanced forensic toolkits usable across the EU an providing comparable results admissible in court;

Long term:

- Path towards an EU-wide certification mechanism based on common standards.

SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories

Topic conditions

- Forensic laboratories or institutes from a minimum of 5 EU Member States or international organisations must be beneficiaries of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant.

Type of action: PCP Pre-Commercial Procurement

Deadline Model: single-stage

Indicative budget: 10M€

Deadline: August 24, 2017

SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks

Challenge: Research has proposed detectors of precursors of explosives, drugs, and more substances threatening the security of the citizens – not yet exploited!

Scope

- Proposals

    - should address the deployment of detection systems in large and medium cities, in existing networks for instance for the detection of explosive precursors and illegal chemicals (drugs).

    - shall address sewage networks and quality of air monitoring networks, and may address other networks. The experiment should last at least two years.

    - should provide a mobile platform equipped to ascertain the location of suspicious measurements.

    - should provide a prototype controlling the detection systems and capable of fusing data provided by a variety of such networks pay particular attention to ethical issues.

- Coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes.

- Proposers for this topic should look for an enhanced SME participation.

- The outcome of the proposal is expected to lead to development up to TRL 7 to 8 for the sensors deployed; 6 for the control and information system, and the mobile platform

SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks

Expected impact

Short term:

- Real-life demonstrations of the combination of systems detecting precursors of explosives, and drugs, installed on at least two utility networks, and making use of a prototype of information systems fusing the data provided by these networks;

- Better understanding of the effectiveness of the combination of technologies used to detect and locate a bomb factory or a drug lab/drug consumption/traffic;

Medium/Long term:

- Provision of a higher level of information/intelligence to those involved in counter-terrorist and countering drugs activities (e.g. Law Enforcement Agencies, Security & Intelligence Agencies, and Government Laboratories)

SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks

Topic conditions

- At least two independent utility network operators; and Law enforcement agencies (LEA) in charge of counter-terrorism, or bomb squad units, from at least 3 EU Members States must be beneficiaries of the grant agreement(Additional participation from LEAs from Associated Countries is encouraged) and should be directly involved in the carrying out of the tasks foreseen in the grant.

- Demonstrations must take place in at least 2 agglomerations: One of over 1,000,000 inhabitants, and another of between 100,000 and 300,000 inhabitants, located in 2 different Member States, and using different types of sewage systems (separating domestic waters from rain waters, or not.).

Type of action: IA Innovation action

Deadline Model: single-stage

Indicative budget: 8M€

Deadline: August 24, 2017

SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

Challenge: LEAs are lagging behind when tackling crime supported by "advanced" technologies.

Scope

- New knowledge and targeted technologies for fighting both old and new forms of crime and terrorist behaviours supported by advanced technologies;

- Test and demonstration of newly developed technology by LEAs involved in proposals;

- Innovative curricula, training and (joint) exercises to be used to facilitate the EU-wide take-up of these new technologies, in particular in the fields of:

  - Sub-topic: 1.cyber-crime: virtual/crypto currencies des-anonymisation / tracing/impairing where they support underground markets in the darknet.

  - Sub-topic: 2.detection and neutralization of rogue/suspicious light drone/UAV flying over restricted areas, and involving as beneficiaries, where appropriate, the operators of infrastructure

  - Sub-topic: 3.video analysis in the context of legal investigation

  - Sub-topic: Others.

- The outcome of the proposal is expected to lead to development up to TRL 6

SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

Expected impact

Short term:

- Improved investigation capabilities;

Medium/Long term:

- Crimes solved more rapidly, to reduce societal distress, investigative costs and the impact on victims and their relatives;

- Prevention of more terrorist endeavours;

- LEA officers provided with better tools to help them on their (specialized) daily work;

- Better identification and understanding of criminal activities

SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

Topic conditions

- In Sub-topic: 1, Sub-topic: 2 or Sub-topic: 3: a minimum of 3 Law enforcement agencies (LEA) from 3 EU Member States or Associated Countries must be beneficiaries of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant.

- In other fields (Sub-topic: "Others"): a minimum of 5 LEA from 5 EU Member States or Associated Countries must be beneficiaries of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant.

- Please note that this topic is planned to be opened also in 2017 with an indicative opening date of 01/03/2017 and an indicative deadline of 24/08/2017, subject to a separate financing decision for 2017

Type of action: RIA Research and Innovation action

Deadline Model: single-stage

Indicative budget: 5M€

Deadline: August 24, 2017

Call - Digital Security Focus Area

- DS-06-2017: Cryptography

- DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors

- DS-08-2017: Privacy, Data Protection, Digital Identities

EUROPEAN COMMISSION

HORIZON 2020

INNOVATION UNION

DS-06-2017: Cybersecurity PPP: Cryptography

Challenge: The improvement of cryptographic solutions is a persistent need across ICT

Scope

Proposals may address one or more of the areas described below (not necessarily all of them):

- Functional encryption solutions that make it feasible to process encrypted data held on the Internet. Research should aim for solutions beyond the current only partial homomorphic encryption algorithms.

- Ultra-weight cryptology for Internet of Things applications, implantable medical devices and sensor nodes that harvest energy from the environment.

- Implementation (hardware or software) is often the weak point of cryptographic protocols. Development of toolkits that integrate encryption seamless in their toolbox environment.

- Authenticated encrypted token research for mobile payment solutions and related applications

- Innovative cryptographic primitives and non-cryptographic mechanisms to enforce privacy at various levels.

- New techniques, such as quantum safe cryptography, which are secure from quantum computers and other advances in computing and cryptanalysis.

- Proposals on quantum key distribution addressing challenges such as improved performance network integration and the development of new protocols beyond key distribution.

- Automated proof techniques for cryptographic protocols.

- The outcome of the proposals is expected to lead to TRL 3 to 5

DS-06-2017: Cybersecurity PPP: Cryptography

Expected impact

- Increase the trustworthiness of European ICT services and products and the competitiveness of the European cryptography and smart card industry.

- Increased trust in ICT and online services.

- Protecting the European Fundamental Rights of Privacy and Data Protection.

- Communication networks with automatic interference detection.

- Improvement in performance and efficiency of cryptography beyond the state of the art.

- Protection against emerging threats such as quantum computation.

DS-06-2017: Cybersecurity PPP: Cryptography

Topic conditions

- No special criteria

Type of action: RIA Research and Innovation action

Deadline Model: single-stage

Indicative budget: 3-5M€

Deadline: April 25, 2017

DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Challenge

- Over the past decade, we have seen that cyber attacks have become increasingly sophisticated, stealthy, targeted and multi-faceted.

- Detecting and responding to such attacks by a highly motivated, skilled and well-funded attacker has however been proven highly challenging.

- As our society is becoming increasingly dependent on (critical) cyber infrastructure, new technologies are needed to increase our detection and response capabilities.

DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Scope

<u>Research and Innovation Actions –Situational Awareness</u>

- The focus of the proposals should be on the development of novel approaches for providing organisations the appropriate situational awareness in relation to cyber security threats allowing them to detect and quickly and effectively respond to sophisticated cyber-attacks.

- The solution may leverage techniques such as anomaly detection, visualisation tools, big data analysis, threat analysis, deep-packet inspection, protocol analysis, etc as well as interdisciplinary research to counter threat actors and their methods.

- The proposals should

    - consider the need to collect necessary forensic information from attackers that can be used as evidence in court.

    - assess and address the impact to fundamental rights, data protection and privacy in particular, in the design and development of their solutions.

- The outcome of the proposals is expected to lead to development up to TRL 3-5.

DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Scope

Innovation Actions – Simulation Environments, Training

- Proposals should develop innovative simulation environments and training materials to adequately prepare those tasked with defending high-risk organisations to counter advanced cyber-attacks.

- The simulation environments should take into consideration the following challenges:

  - Tools for creating realistic cyber environments that fit the training objectives and tools for producing both benign and malicious system events that fit the training scenario;

  - Real-time student performance assessment, dynamic configuration and adaptation of exercise scope and difficulty;

  - Exercise monitoring and evaluation of its state, being able to control the progress of the exercise, detect inconsistencies and hard-to-solve situations, etc;

  - Definition and creation of new scenarios and cyber threats in a cost and time-effective manner, and that better achieve the pedagogical objectives for a wide variety of student profiles;

- For cyber security attacks, proposals may also consider scenario building and simulation training to prepare organisations' response and decision making processes in relation obligations stemming from applicable legal frameworks or in the wider context of managing crises and emergency situations.

- The outcome of the proposals is expected to lead to development up to TRL 6 to 7

- Proposals have to address the specific needs of the end-user, private and public security end users alike.

- Proposals are encouraged to include public security end-users and/or private end users

DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Expected impact

- Improved detection and response time to advanced cyber security threats.

- Increase society's resilience to advanced cyber security threats.

- (RIA) Progress in technologies and processes needed to improve organisations' capabilities to detect and respond to advanced attacks.

- (IA) Improvements in the preparedness of those charged with defending ICT systems from advanced threats in high risk scenarios.

DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Topic conditions

- No special criteria

Type of action: RIA Research and Innovation action & IA Innovation action

Deadline Model: single-stage

Indicative budget: RIA: 2-3M€, IA: 4-5M€

Deadline: August 24, 2017

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Challenge

- The use of modern telecommunications and on-line services involve users' personal information. For example
  - using search engines exposes the query terms used, which can be both sensitive and identifying, as illustrated by the exposure of search terms
  - social networking services expect users to reveal their social connections, messages and preferences, that could lead to direct privacy violation if exposed.

- The implementation the draft General Data Protection Regulation presents both technological and organisational challenges for organisations
  - They have to implement novelties such as the right to data portability, the right to be forgotten, data protection impact assessments

- Many services on the Internet depend on the availability of secure digital identities which play a crucial role in safeguarding the data and privacy of citizens

- Many European countries already have / are in the process of developing an electronic identity (eID) scheme.

- Most of these schemes have a very high security level, which makes them very suitable for diverse eGovernment processes but they lack usability for commercial applications.

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Scope

Proposals may cover one of the strands identified below.

- <u>Privacy-enhancing Technologies (PET)</u>

    - Novel designs and tools to provide users with the functionality they require without exposing any more information than necessary, and without losing control over their data, to any third parties.

    - Comprehensive and consistent Privacy Risks Management Framework

    - Open source and externally auditable solutions

- <u>General Data Protection Regulation in practice</u>

    - Tools and methods to assist organisations to implement the GDPR taking into account the final provisions of GDPR and guidance from relevant authorities

    - Proposals may also address the need to provide support (procedures, tools) for entities to understand how to operate without requiring unnecessary information (so as to promote privacy respecting practices).

- <u>Secure digital identities</u>

    - With a view to reducing identity fraud while protecting the privacy of citizens, proposals should develop innovative, secure and privacy enhancing digital identity platforms beyond national eID systems.

    - Activities may leverage existing European electronic identification and authentication platforms with clearly defined interfaces based on the General Data Protection Regulation (GDPR).

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Scope

- For all strands, proposals should identify and address the societal and ethical dimensions of the strand they choose to cover taking into consideration the possibly divergent perspectives of pertinent stakeholders.

- Proposals have to address the specific needs of the end-user, private and public security end users alike. Proposals are encouraged to include public security end-users and/or private end users.

- The outcome of the proposals is expected to lead to development up to TRL 6 to 7.

This project is co-financed by the European Union and the Republic of Turkey
Bu proje Avrupa Birliği ve Türkiye Cumhuriyeti tarafından finanse edilmektedir

EUROPEAN COMMISSION

HORIZON 2020

INNOVATION UNION

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Expected impact

- Support for Fundamental Rights in Digital Society.

- Increased Trust and Confidence in the Digital Single Market

- Increase in the use of privacy-by-design principles in ICT systems and services

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Topic conditions

- No special criteria

Type of action: IA Innovation action

Deadline Model: single-stage

Indicative budget: 2-3M€

Deadline: August 24, 2017

Thanks for your attention!